Derivation of Failure Rates and Probability of Failures for the International Space Station Probabilistic Risk Assessment study

Dr. Roberto Vitali
Futron Corporation
Bethesda, Maryland USA

Michael G. Lutomski
NASA – Johnson Space Center
Houston, Texas USA

1 Introduction

National Aeronautics and Space Administration's (NASA) International Space Station (ISS) Program uses Probabilistic Risk Assessment (PRA) as part of its Continuous Risk Management Process. It is used as a decision and management support tool to not only quantify risk for specific conditions, but more importantly comparing different operational and management options to determine the lowest risk option and provide rationale for management decisions.

This paper presents the derivation of the probability distributions used to quantify the failure rates and the probability of failures of the basic events employed in the PRA model of the ISS. The paper will show how a Bayesian approach was used with different sources of data including the actual ISS on orbit failures to enhance the confidence in results of the PRA. As time progresses and more meaningful data is gathered from on orbit failures, an increasingly accurate failure rate probability distribution for the basic events of the ISS PRA model can be obtained.

1.1. The International Space Station PRA Model

The ISS PRA has been developed by mapping the ISS critical systems such as propulsion, thermal control, or power generation into event sequences diagrams and fault trees. The lowest level of indenture of the fault trees was the orbital replacement units (ORU). The ORU level was chosen consistently with the level of statistically meaningful data that could be obtained from the aerospace industry and from the experts in the field. For example, data was gathered for the solenoid valves present in the propulsion system of the ISS. However valves themselves are composed of parts and the individual failure of these parts was not accounted for in the PRA model. In other words the failure of a spring within a valve was considered a failure of the valve itself.

2 Bayesian Updating or Probability Distributions of Failure Rates

2.1 Basic Events

The basic event is at the lowest level in system breakdown at which significant statistical information is available, typically in the form of failure rates. Typically, with exceptions, the lowest level modeled in this ISS PRA is the ORU level. The ORU level is chosen because basic events can describe failure modes, repair events, or common cause failures. Once quantified the basic event's probability of failure propagates upwards through the fault tree of the system to calculate the probability of occurrence of the top event via Boolean logic.

The ISS PRA uses a linked fault tree/event tree methodology to ultimately calculate the probability of an undesired event from the probabilities of the basic events. In addition to the quantification of the end states the hierarchical structure of the PRA allows for the evaluation of the factors leading to those the undesired states.

2.1 Deriving Data to Quantify Basic Events

The approach to derive data to quantify basic events starts when possible with industry available database tracking failures such as NPRD (Non-electrical Parts Reliability Database) and EPRD (Electrical Parts Reliability Database) as well as the ISS program own database MADS. The data obtained from the databases is than treated as detailed in the following sections and than periodically updated with failures observed on orbit through the use of Bayesian methods. The quantification of the basic events was therefore completed in two phases as shown in the flowchart of Figure 1.

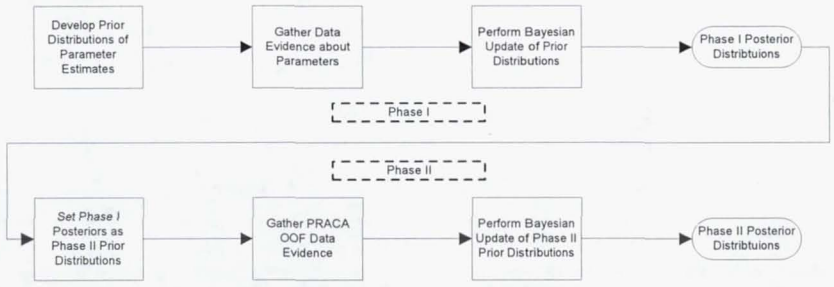

Figure 1: Basic event quantification flowchart

3 ISS PRA Model Data Derivation

The quantification of the ISS PRA parameters progressed in two phases. During the first phase (Phase I in Figure 1) component/ORU were divided in four categories electronics, electrical, mechanical, and electro-mechanical and a prior distribution

for each of the four categories was derived. Examples of components respectively belonging to each category are A/D converters, Remote Power Control Module (RPCM), electro-mechanical valves, and pyro-valves. The priors were than updated using a Bayesian procedure with data obtained for each ORU from different sources and databases. Evidence came in the form of number of failures per an operation time, number of failures per number of demands, failure rates, mean time between failures (MTBF), and estimates of the probability of failure (POF).

Phase II started by using the results of Phase I as prior and updated the parameter distributions obtained during the first phase by including failures experiences on orbit and captured by the PRACA database developed by NASA. The information about on orbit failures included in Phase II updating procedure was obtained by searching the PRACA database. The last update performed was carried out with failures recorded on orbit until October 31st 2003. The Bayesian updating procedures were carried out using ReDat [1] software developed by Prediction Technologies in collaboration with the University of Maryland.

3.1 Phase I Posterior Distributions

The first stage in Phase I of the updating process derived the expression for suitable prior distributions. It was agreed that since the ISS contains such a diverse group of component classes, prior distributions would be based on broad categories of components. Through utilizing data gathered from the Space Station Freedom External Maintenance Task Team (EMTT) Final Report [?], prior distributions of both the failure rates and probabilities of failure were developed for classes of components that were electronic, electrical, electro-mechanical, and mechanical.

3.1.1 Failure Rate Distributions

A key assumption made in utilizing the EMTT study to derive failure rates utilized as prior distributions was that distributions obtained from the EMTT study were lognormal distributions. The lognormal distributions were calculated by fixing the 5th and 95th percentiles of the reported failure rate distributions from the EMTT study. Setting the 5% and the 95% percentiles uniquely defined every lognormal distribution. Table 1 below show the resulting lognormal prior failure rate distributions.

	5th%	Mean	95th%
Electronics	2.00E-07	2.50E-06	1.00E-05
Electrical	1.50E-08	3.00E-06	1.20E-05
Electro-Mechanical	2.00E-08	2.50E-05	7.00E-05
Mechanical	2.00E-08	2.00E-05	7.00E-05

Table 1: Failure Rate Data Obtained from EMTT Study for the four Component Classes per hour

3.1.2 Probability of Failure Distributions

Having defined the probability distribution for the failure rates does not define the probability of failure. As mentioned in the ISS PRA study it was assumed the all the failure rates were independent of time. The probability of failure distributions for a constant failure rate system can be modeled using the exponential reliability equation [3]:

$$P_o(\lambda) = 1 - e^{(-\lambda t)} \qquad (1)$$

where λ indicates the probabilistic failure rate and *t* is the operating time. In order to calculate the probability of failure distribution functions the probability distribution function of λ were used in Eq. 1 and Monte Carlo simulations typically using 10,000 sample points were run to derive an histogram for the distribution function of $P_0(\lambda)$. From the resulting histogram the 5% percentile and the 95% percentile were fixed as the 5% and the 95% percentiles of a corresponding lognormal distribution. The lognormal distribution obtained was used to represent the probability of failure. Verifications on the accuracy of lognormal distribution were performed by calculating the error factor (EF) of the histogram in two forms. The EF calculated from median and the 5% percentile was compared with the EF calculated from the 95% and the median of the histogram. In all the case encountered the computed EFs did not differ significantly indicating a lognormal distribution was a good fit. Table 2 below show the resulting lognormal prior probability of failure distributions for the four categories of hardware.

	5th%	Mean	95th%
Electronics*	4.90E-04	6.10E-03	2.00E-02
Electrical*	3.20E-05	7.00E-03	2.50E-02
Electro-Mechanical*	4.80E-05	2.50E-02	1.20E-01
Mechanical*	4.90E-05	2.80E-02	1.40E-01

Table 2: Probability of failure Obtained from EMTT Study for the four Component Classes and Monte Carlo simulation for six months of operation time

3.1.3 Demand Based Probabilities of Failure

Probabilities of failure per demand were often computed from the failure rates of the component when operating. It was assumed that when data to quantify the probability of failure per demand was not readily available if the device failed to operate when demanded it failed while in a "dormant" or idle phase. The failure rate of the device when idle was assumed to be,

$$\lambda_d = \frac{\lambda}{10} \qquad (2)$$

where λ_d in Eq. 2 indicates dormant failure rates and λ indicates operational failure rates.

3.1.4 Data Evidence

The second stage in Phase I of the data derivation consisted in updating the four general component categories with component specific data found from several sources. In general the probability distribution of the failure rates were updated with a Poisson likelihood functions that is well suited to describe the number of failures occurred in during the time of operation. The updating procedure was again carried our using the ReDat software developed by the University of Maryland.

3.1.5 Data Sources

As with the prior distributions, several assumptions were made in gathering data evidence. First, it was assumed that the only pertinent data sources for this study were the ISS Program's MADS database as well as the Reliability Analysis Center's (RAC) NPRD and EPRD databases. Other data sources (Bellcore, etc) were also consulted when no other data was available in MADS, NPRD and EPRD. The data source was restricted to RAC and MADS to avoid double counting. A second assumption was that when the data encountered was in the form of failure rate (vs. actual failures and the time of operation) it represented the *median* of the failure rate of the component/ORU being quantified.

3.1.6 Space Environment Conversion Factor

The information obtained from the RAC databases were already inclusive of a space environment conversion factor (SEC). The SEC factor converts the number of failures (k) during a specified time (t) that the component/ORU experiences in its native environment, to the number of failures that would have been observed in space. For example, given 10 failures in 100,000 hours, and an SEC of 2, the resulting adjusted number of failures would be 5 failures in 100,000 hours.

3.1.7 Posterior Distributions

The final stage of Phase I of the updating process enabled the output of meaningful posterior distributions of the failure rate or probability of failure for the ISS components/ORUs. Again, several underlying assumptions were made in order to perform the Bayesian updates. First, it was assumed that the failure behaviour of all components/ORUs, unless noted otherwise was distributed lognormal. Thus the resulting posterior distributions were set as lognormal distributions using the mean and EF values.

3.2 Phase II - PRACA Data Incorporation

Phase II of the Bayesian update utilizes a second and perfectly applicable source of data. This data is collected from the PRACA OOF database of actual component/ORU failures experienced on the ISS. By performing some simple data analyses, the PRA team has been able to build a database which lists the components/ORUs that have or have not failed. This information is easily incorporated into the Bayesian updating process. Since on-orbit data is yielded from the systems being modeled, given enough time of operation it does not matter how

broad the prior distributions are (as is the case with the EMTT prior distributions), the on orbit data will drive the posterior distributions closer to their true values. In other words as more information on the behavior of the components on orbit accumulates the relative importance of the priors diminishes.

Phase II begins after the PRACA OOF data has been collected and is input into the ReDat tool to perform the Bayesian updating. One thing to note is that even if a component/ORU does not experience a failure during the time for which OOF data is recorded, the distribution is still updated with zero failures.

Just as the Phase I prior distributions could be updated with failure per time of operation data, Phase II priors (the posteriors yielded from Phase I) were also updated using a Poisson likelihood function for the data derived from PRACA OOF. The resulting distributions were assumed to be lognormal. In some instances the available data from on orbit operation was so overwhelming that the result of the Bayesian updating procedure was a single value. The inclusion of failures from the PRACA OOF database was updated for the last time as October 31st 2003.

4 Conclusion

This paper demonstrates an approach for deriving the data for the basic events used in the ISS PRA. The methodology used with ISS PRA seeks to give the Space Station program an accurate view of the risk picture inherent in the overall Station system. The processes adhered to by the PRA analysts progressively incorporated the most up-to-date, reliable, and applicable information available. Indicative of this is the use of the Station program's MADS database for the MTBFs of the Station components/ORUs.

This is one of the first applications in the aerospace industry to incorporate this technique using industry available data, expert opinion, and on orbit failures. This method of deriving the data for the basic events using Bayesian updating to the distributions has provided vastly improved analysis results from the ISS PRA model. It is our hope that even with major refinements this technique will serve as a benchmark for future PRA studies in the aerospace industry.

References

1 Reliability data collection and analysis tool (ReDat), prediction technologies, 2002

2 Fisher and Price, Space Station Freedom External Maintenance Task Team (EMTT) Final Report Volume I Part II, July 1990

3 Villemeur, Alain. *Reliability, Availability, Maintainability, and Safety Assessment*, Vol. 1. John Wiley & Sons Ltd, West Sussex, England, 1992.